What's New in Directory Services

Session 614

These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

What’s New in Directory Services

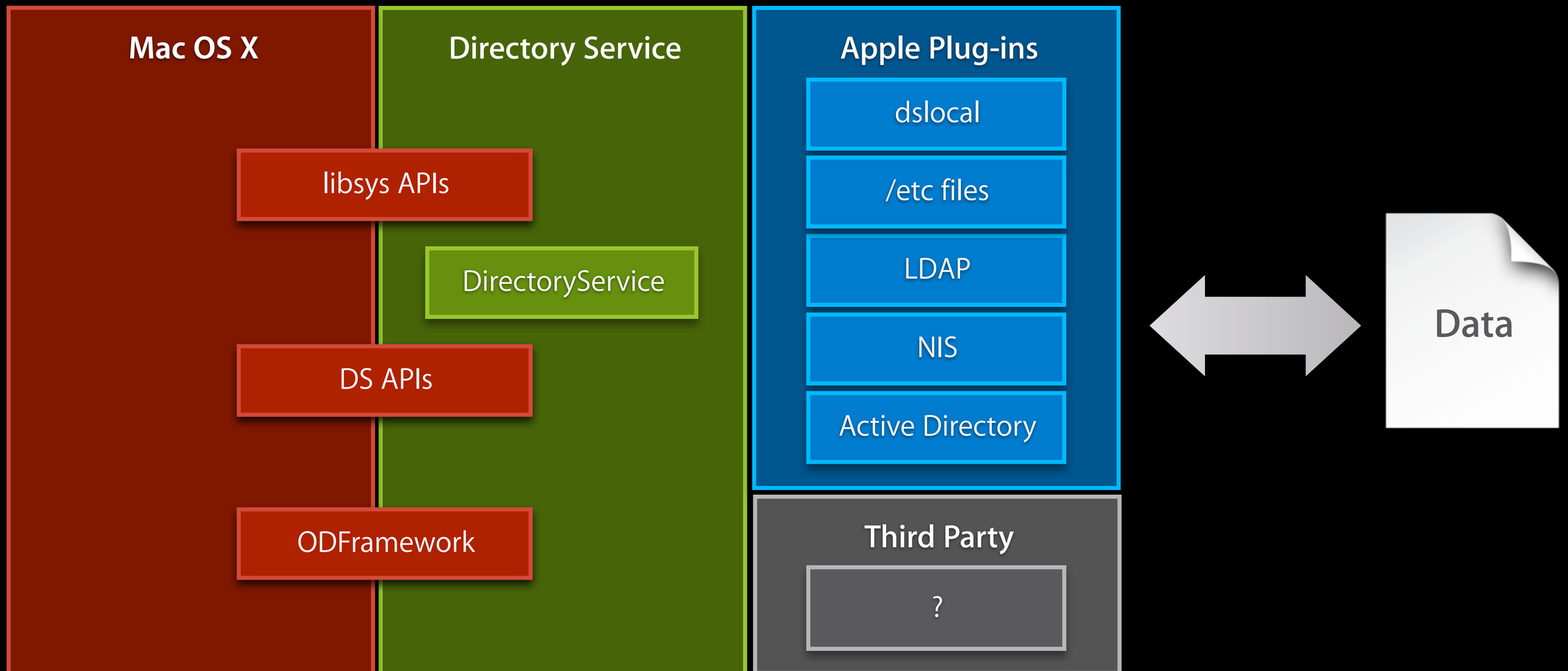
Nicole Jacque
Directory Server Engineering

Agenda

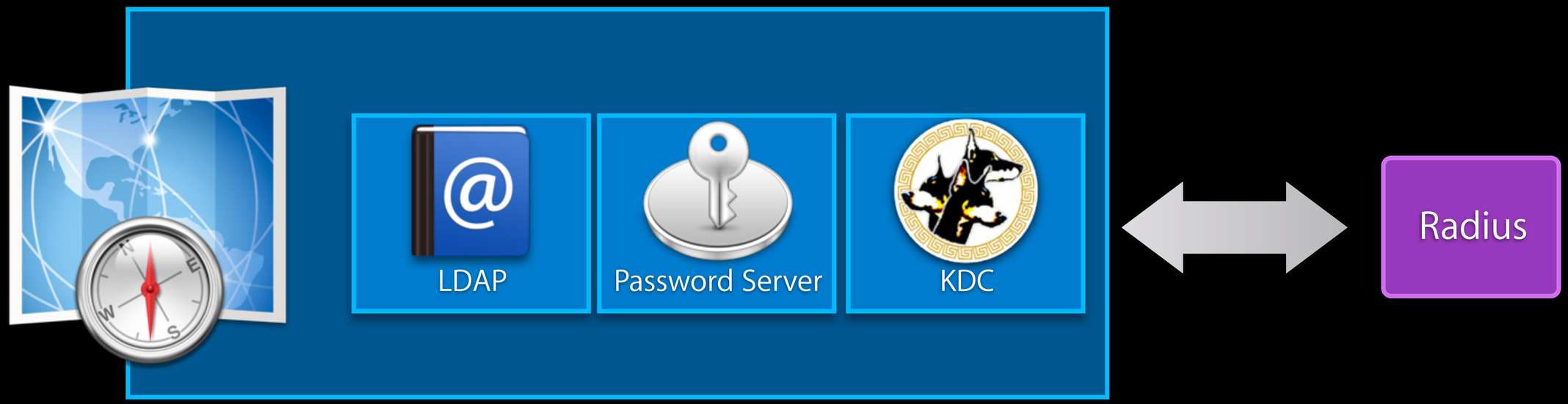
- Overview
- DirectoryService
- Active Directory Plugin
- Open Directory
- Best Practices

Overview

OS X Directory Service Client

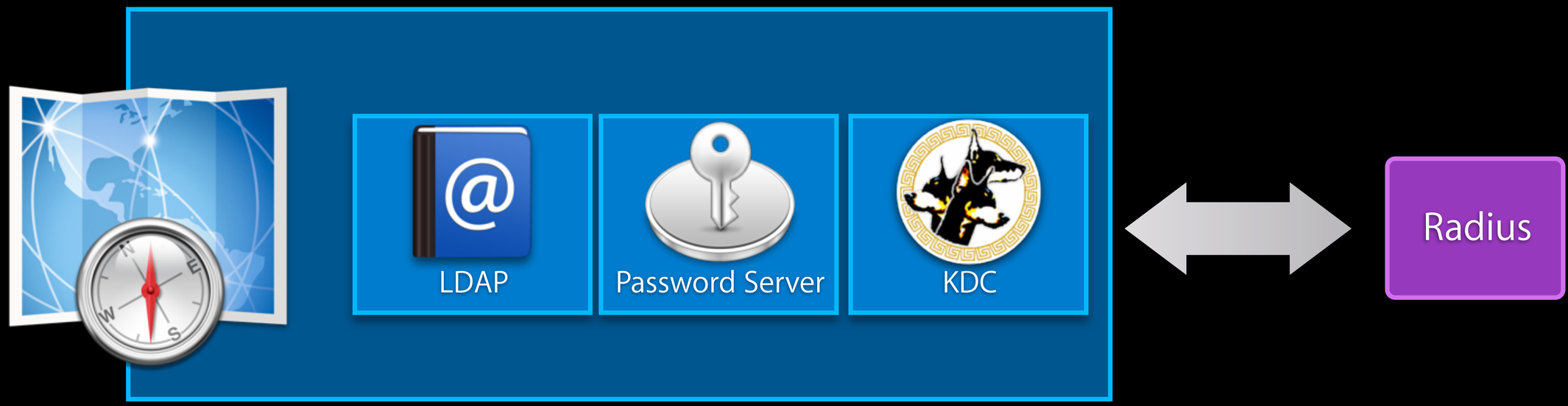


Open Directory Server



Open Directory Server

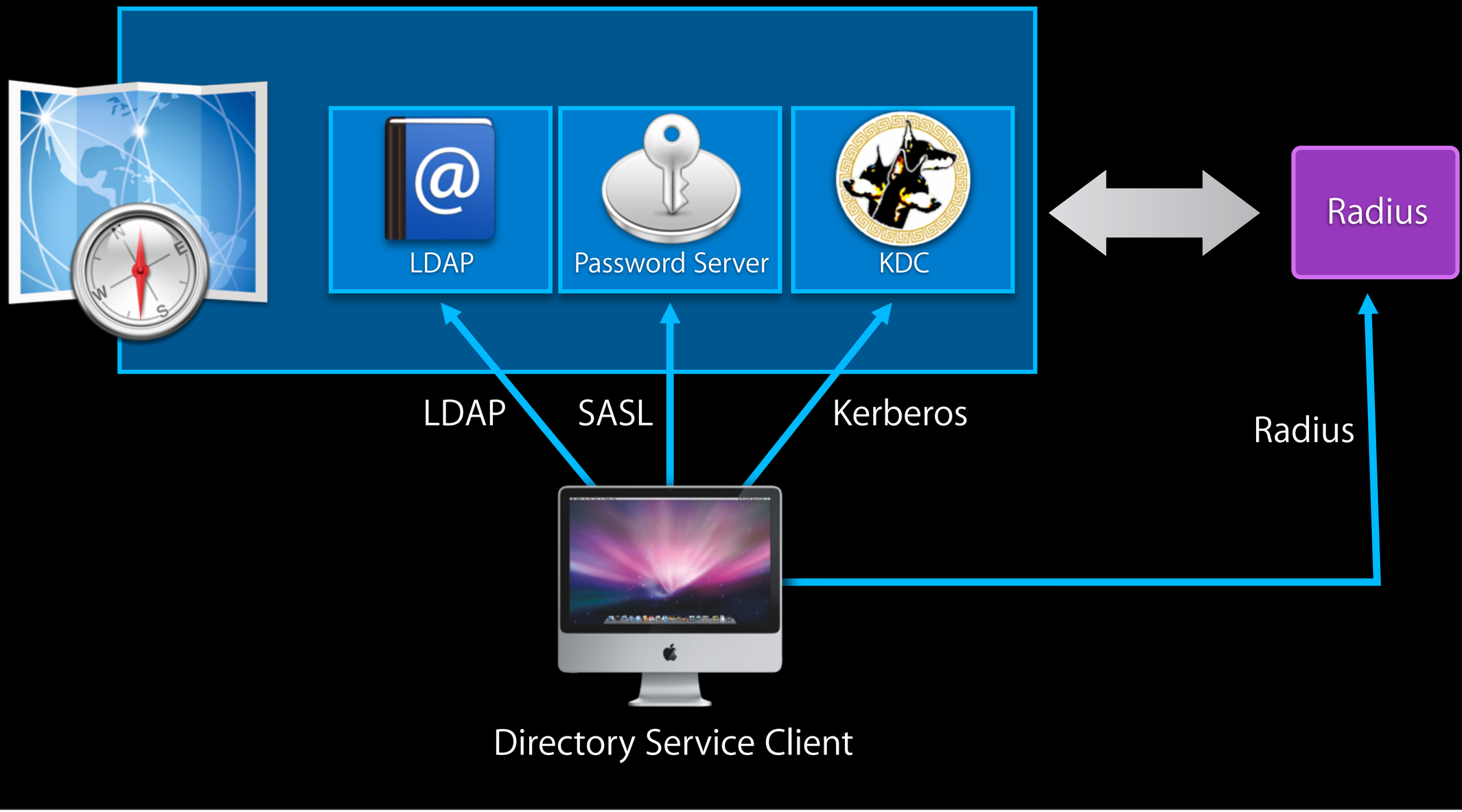
Clients can use Directory Service Client



Directory Service Client

Open Directory Server

Standard protocols supported



Directory Service in Snow Leopard

10.6—Evolution

- Code cleanup
- Efficiency and performance
- Bug fixes

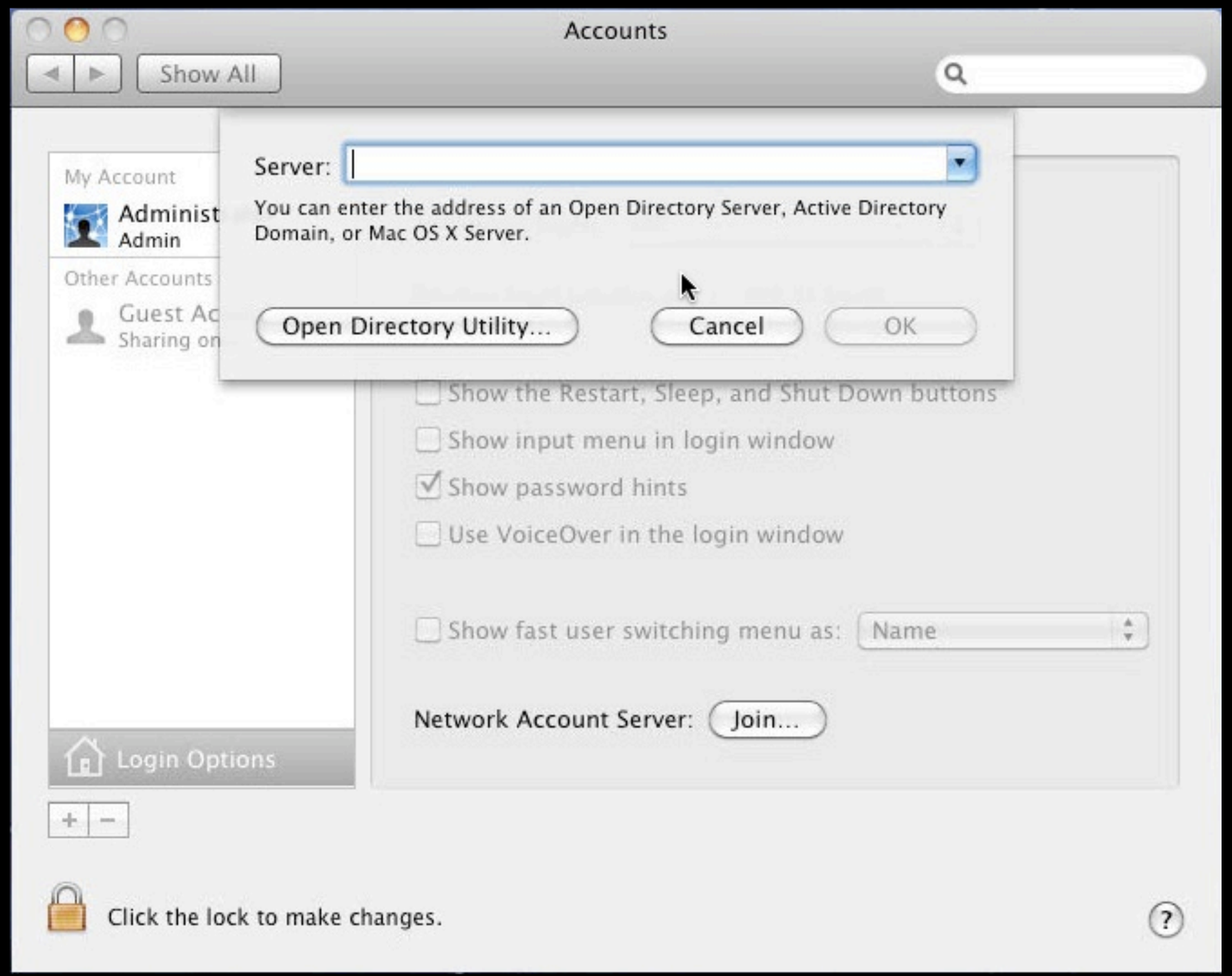
UI Changes

- Simplified UI for binding in System Preferences

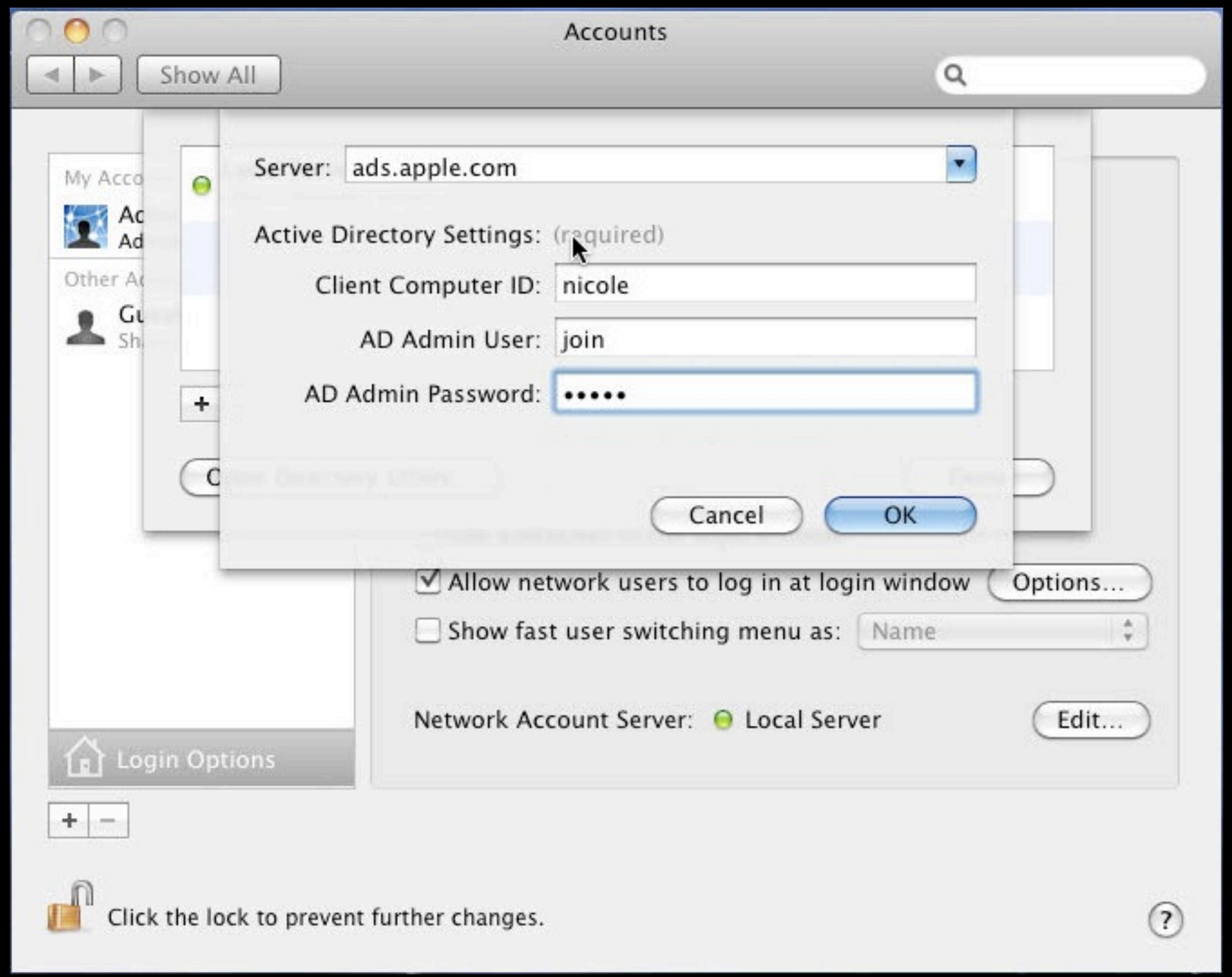
UI Changes

Accounts
Show All
My Account
Administrator
Admin
Other Accounts
Guest Account
Sharing only
Login Options
Automatic login:
Off
Display login window as:
List of users
Name and password
Show the Restart, Sleep, and Shut Down buttons
Show input menu in login window
Show password hints
Use VoiceOver in the login window
Show fast user switching menu as:
Name
Network Account Server:
Join...
Click the lock to make changes.

UI Changes


Accounts
Show All
Server:
You can enter the address of an Open Directory Server, Active Directory Domain, or Mac OS X Server.
Open Directory Utility...
Cancel
OK
My Account
Administ
Admin
Other Accounts
Guest Ac
Sharing on
Show the Restart, Sleep, and Shut Down buttons
Show input menu in login window
Show password hints
Use VoiceOver in the login window
Show fast user switching menu as:
Name
Network Account Server:
Join...
Login Options
Click the lock to make changes.

UI Changes

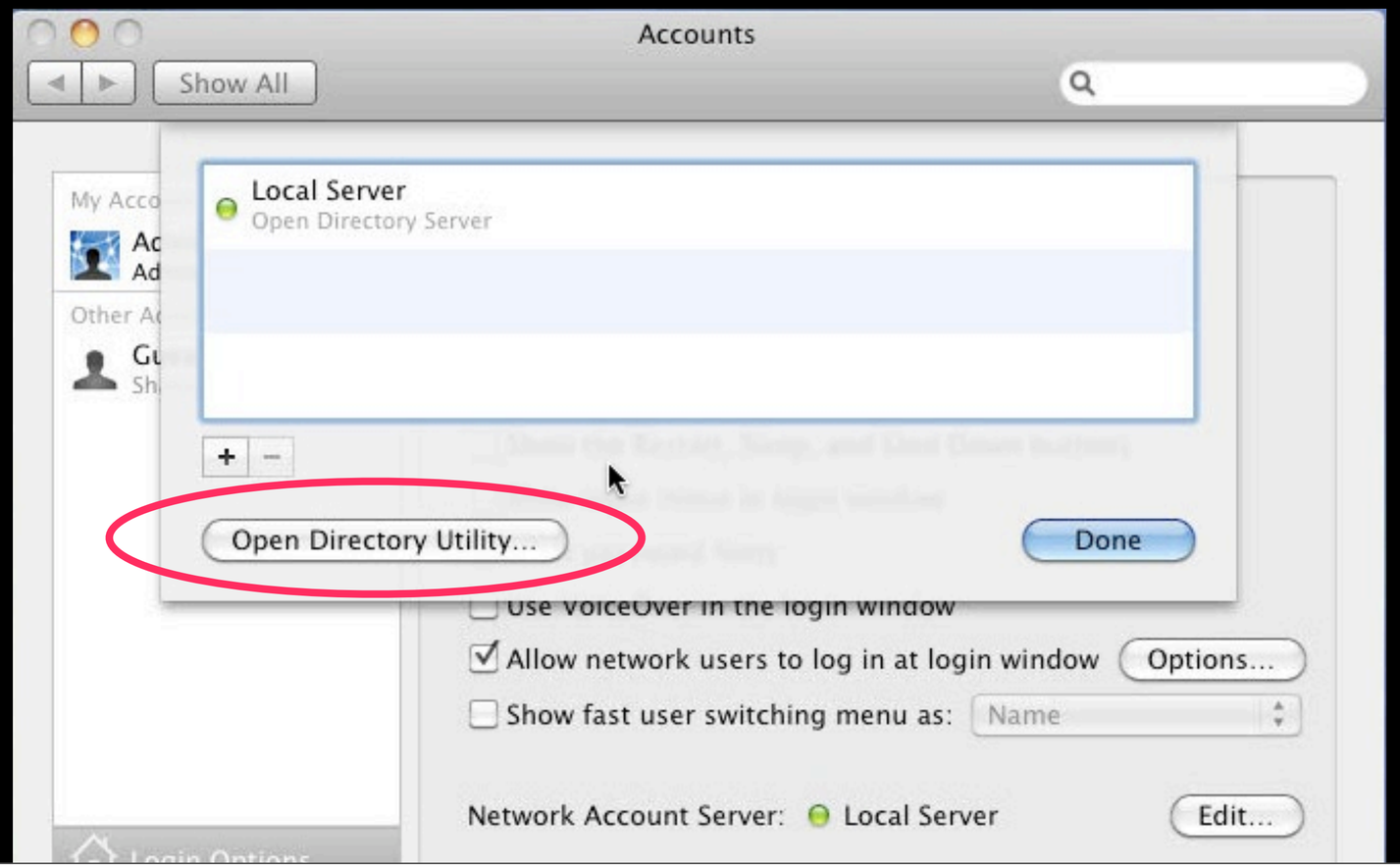

Accounts
Show All
Server: ads.apple.com
Active Directory Settings: (required)
Client Computer ID: nicole
AD Admin User: join
AD Admin Password: •••••
Cancel
OK
Allow network users to log in at login window
Options...
Show fast user switching menu as: Name
Network Account Server: Local Server
Edit...
Login Options
Click the lock to prevent further changes.

UI Changes

Accounts
Show All
ads.apple.com
Active Directory Domain
Open Directory Utility...
Done
Use VoiceOver in the login window
Show fast user switching menu as:
Name
Network Account Server:
ads.apple.com
Edit...
Login Options
Click the lock to prevent further changes.

UI Changes

- Directory Utility still accessible for more complex binding requirements
  - Lives in /System/Library/CoreServices



Under the Hood

- Adopted GCD (Grand Central Dispatch)
- Deprecated DS API
- Introduced OpenDirectory Framework
- Improved caching
- DNS lookups now handled by mDNSResponder

Active Directory Plugin

Active Directory Plugin Improvements

- Bug fixes
- Better support for common configurations
- Support for Windows Server 2008
- Improved stability
- Better mobility behavior

AD Plugin Changes

Password expiration notices at login

AD Plugin Changes

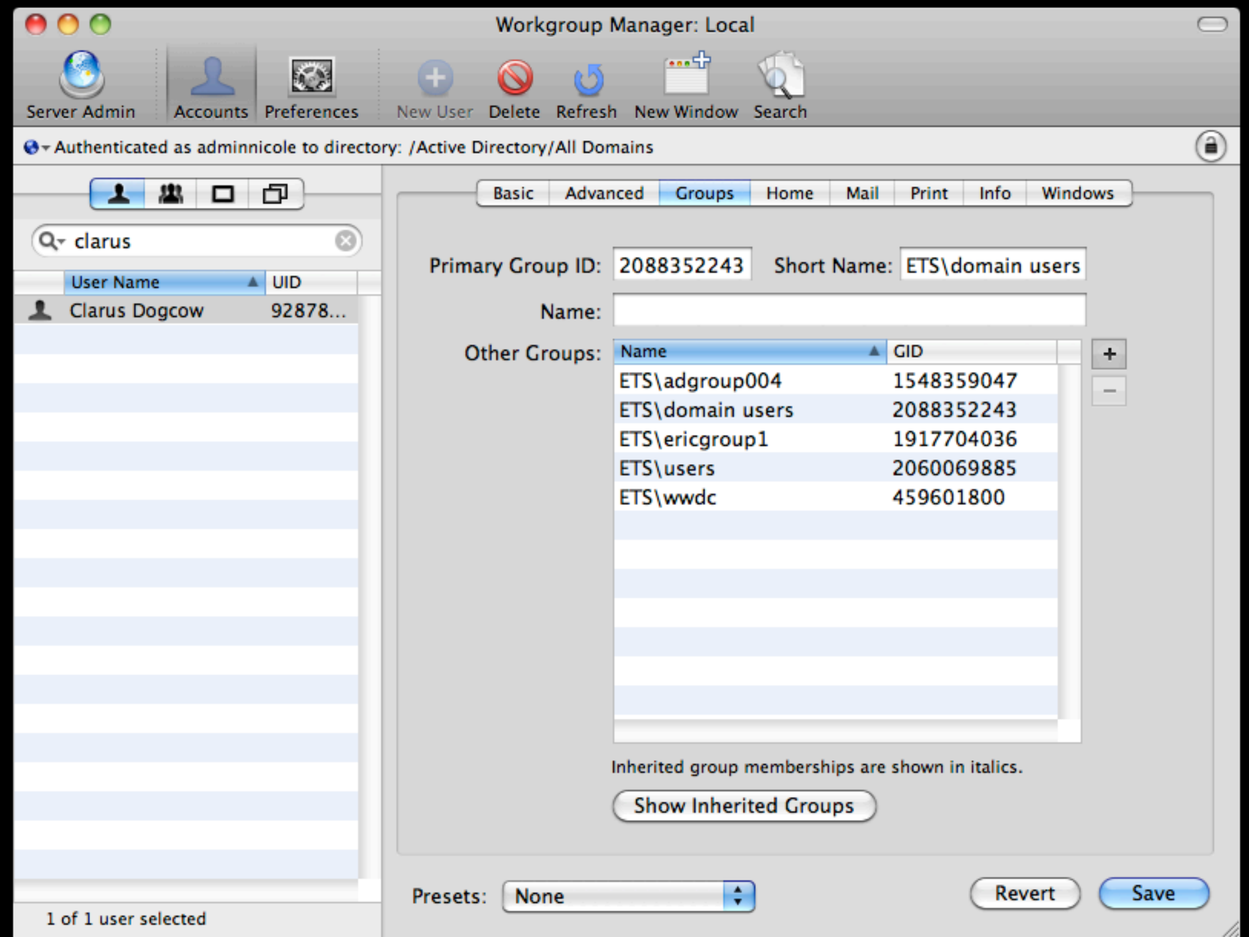
Support for disjointed AD namespaces

```
root% klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   0 host/nicole.ads.apple.com@ADS.APPLE.COM
   0 host/nicole.ads.apple.com@ADS.APPLE.COM
   0 host/nicole.ads.apple.com@ADS.APPLE.COM
   0 nicole$@ADS.APPLE.COM
   0 nicole$@ADS.APPLE.COM
   0 nicole$@ADS.APPLE.COM
   0 host/nicole.apple.com@ADS.APPLE.COM
   0 host/nicole.apple.com@ADS.APPLE.COM
   0 host/nicole.apple.com@ADS.APPLE.COM
```

AD Plugin Changes

Improved Workgroup Manager support

- Editing AD now supports editing
  - Groups
  - Computer lists
  - Existing AD records



AD Plugin—Other Changes

- No querying for macAddress if it's not part of the computer object class
- Differentiate between users and contacts
- Support for IPv6 AD domains
- Support for 3 level+ domains
- Better kerberos support for 2k8 domains

Supporting AD Users in OS X Services

- Augment records no longer needed
  - ServicesLocator attribute requirement has been removed
- Added AD Digest authentication for some services
  - Podcast Producer
  - iChat

Open Directory Server

Open Directory Server

- Performance and scalablity
- Interoperability
  - Better support for “magic triangle” configuration

Server Setup Changes

Users and Groups

Select how you would like to manage users and groups on your server.

Create Users and Groups
Use Open Directory to create users and groups for a small business or home office.

Import Users and Groups
Import users and groups from a directory server on an existing network.

Configure Manually
View more advanced options for configuring directory services.

Go Back Continue ?

Service Access Control Lists (SACLS)

Server Admin: gonzo.local: Server

SERVERS
- Available Servers (182)
- Ready for Install (1)
- Ready for Setup (3)
- gonzo.local

Overview | Logs | Graphs | File Sharing | Server Updates | Certificates | Access | Settings

Services | Administrators

For all services
For selected services below:

Service
Address Book
AFP
Blog
FTP
iCal
iChat
Login Window
Mail
Podcast Producer
QuickTime Streaming
RADIUS
SMB
SSH
VPN
Xgrid

Service access is restricted

Allow all users and groups
Allow only users and groups below:

Name
Administrators

+ −

+ | ⚙ | ↻ | Revert | Save

Service Access Control Lists (SACLS)

- Turned on by default except in manual configuration
- Users automatically added to SACLs in Server Preferences
  - Must manually add users to SACL if created in Workgroup Manager

Directory Services

Set up an Open Directory master to provide network users and groups, as well as other directory services from your server.

Set up an Open Directory master

Directory Administrator

Name: Directory Administrator

Short Name: diradmin UID: 1000

Password: <same as local administrator>

Restrict individual user and group access to services

Service access can be changed using Server Admin or Server Preferences.
Users added in Server Preferences will initially be granted access.

Go Back Continue

Setup Changes—Admin Account

Leopard

Open Directory	server setup admin
Local	Local Administrator (locadmin)

Setup Changes—Admin Account

Snow Leopard

Open Directory	Directory Administrator (diradmin)
Local	server setup admin

LDAP Improvements

- Upgraded to OpenLDAP 2.4.11
- 2x read performance improvement
- syncrepl for LDAP replication

LDAP Improvements

- Removed 1000 connection limit
  - Have tested with over 8000 connections
  - Limited by number of open files allowed
    - One connection = one file

slapd Connection Limit

- Configurable in slapd launchd plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Disabled</key>
        <false/>
        <key>HardResourceLimits</key>
<dict>
        <key>NumberOfFiles</key>
        <integer>8192</integer>
</dict>
<key>Label</key>
<string>org.openldap.slapd</string>
<key>OnDemand</key>
<false/>
<key>Program</key>
<string>/usr/libexec/slapd</string>
<key>ProgramArguments</key>
<array>
        <string>/usr/libexec/slapd</string>
        <string>-d</string>
        <string>0</string>
        <string>-h</string>
        <string>ldap:/// ldapi://%2Fvar%2Frun%2Fldapi</string>
</array>
<key>ServiceIPC</key>
```

LDAP DB Reliability

- Updated version of Berkley DB (BDB)
- Tuned db parameters
- f_fullsync

Reliability vs. Performance

- f_fullsync
  - Good for DB
  - Slower writes
- LDAP operations are mostly reads

Controlling Fullsyncs

- For large imports
  - `slapconfig –setfullsyncmode yes|no`
  - yes = fullsync on normal operation
  - no = fullsync off–during imports

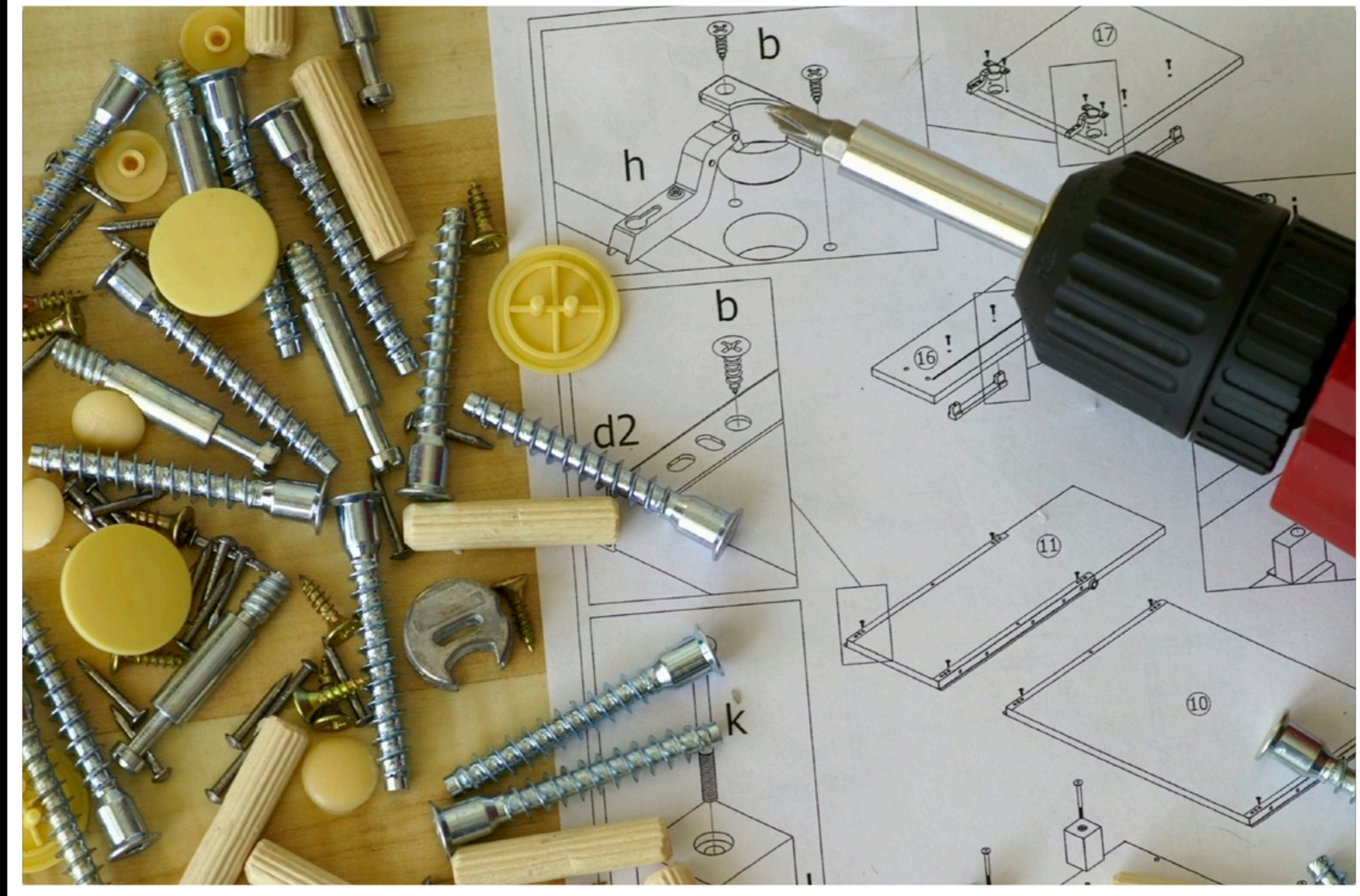
Controlling Fullsyncs

- Don’t run with fullsync off except when importing!
  - Little performance benefit
  - Puts data at risk!

New Features in PasswordServer

- Password synchronization plugin
- Custom password filters

Some Assembly Required



Password Filters

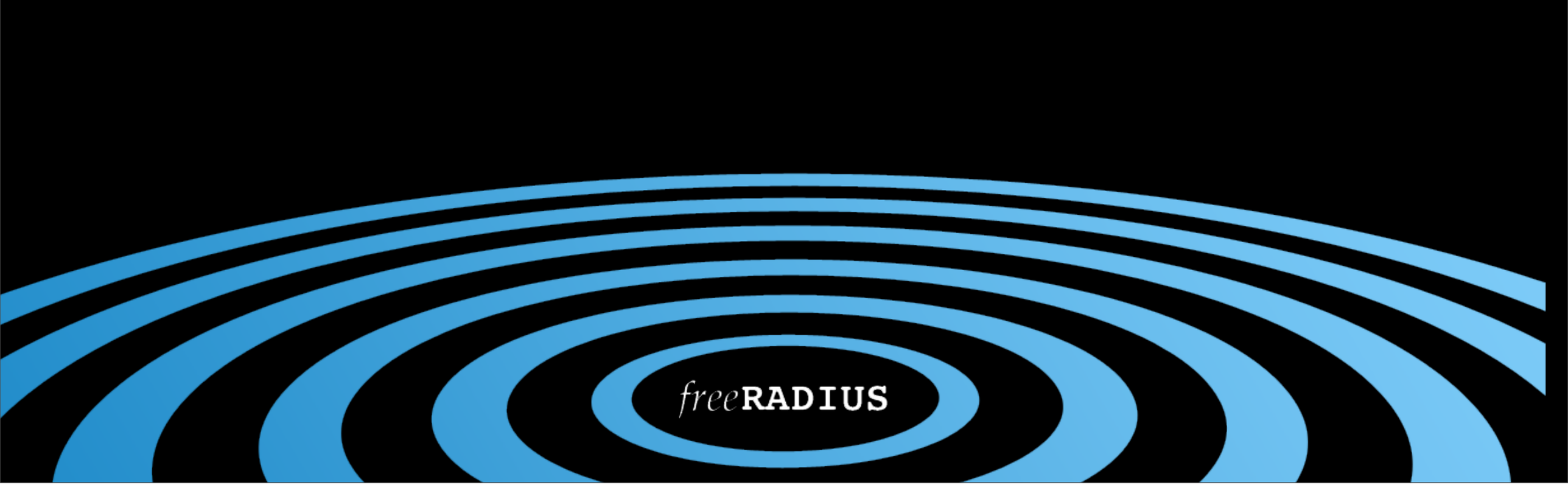
- You write a script or tool
- Install in /Library/Password Server Filters

Writing a Password Filter

- Implement two arguments
  - Preflight: -p
  - Successful change: -c
- XML containing info about user, password, and user type will be passed on stdin
- Exiting nonzero on the preflight will reject the password change

Radius

- Upgraded to FreeRadius 2.1.3
- New: Authentication for AD users



Support for IP/hostname Changes

- Serverwide improvement for changing hostname or IP address
- New tool for changing directory data: changeDirData.pl

```
changeDirData.pl -s server.domain.com -u diradmin -o oldhost.domain.com -n newhost.domain.com -r users
```

Terminal — ssh — 195×49

```
changeDirData.pl(8)       BSD System Manager's Manual      changeDirData.pl(8)

NAME
     changeDirData.pl -- Mac OS X Server OpenDirectory LDAP find/replace tool

SYNOPSIS
     changeDirData.pl [-hiPv] -s server -u diradmin [-p password] -o oldValue -n newValue -r recordType

DESCRIPTION
     changeDirData.pl Searches an Open Directory LDAP server for a specified value, and replaces it.  This is particularly useful for bulk changing record values when a server
     hostname or ip number changes.

     changeDirData.pl should be run against the Open Directory master -- not an Open Directory Replica, but the script itself can be run from any machine on the network.

     It is highly recommended that you make a backup of your directory data (via Server Admin or slapconfig) before making bulk changes.

OPTIONS
     The following options are available:

     -h    prints a usage statement and exits

     -i    The find and replace operation will be done case insensitively.  mysearchstring will match not only mysearchstring, but also  MYSEARCHSTRING and mYsearchSTring

     -v    prints more status information as the script runs

     -s server
           the DNS or IP address of the OD LDAP server

     -u username
           Username for a directory administrator on the LDAP server

     -o oldValue
           the value to search for and replace.
```

Best Practices

Best Practices

- Extending the AD schema
- OpenDirectory topology
- Magic Triangle setup
- Changing your IP or hostname

Extending the AD Schema

Demo

Extending the Active Directory with ADAM

Documentation

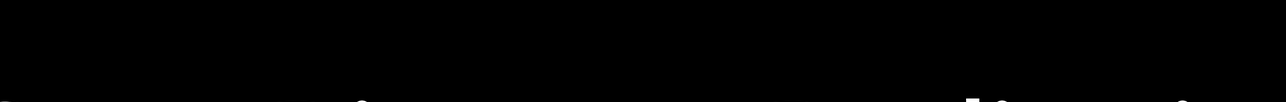
- Whitepaper
  - http://www.seminars.apple.com/seminarsonline/modifying/apple
- Microsoft
  - http://www.microsoft.com/windowsserver2003/adam/default.mspx

Open Directory Topology

Open Directory Replication

1 Master

32 Replicas

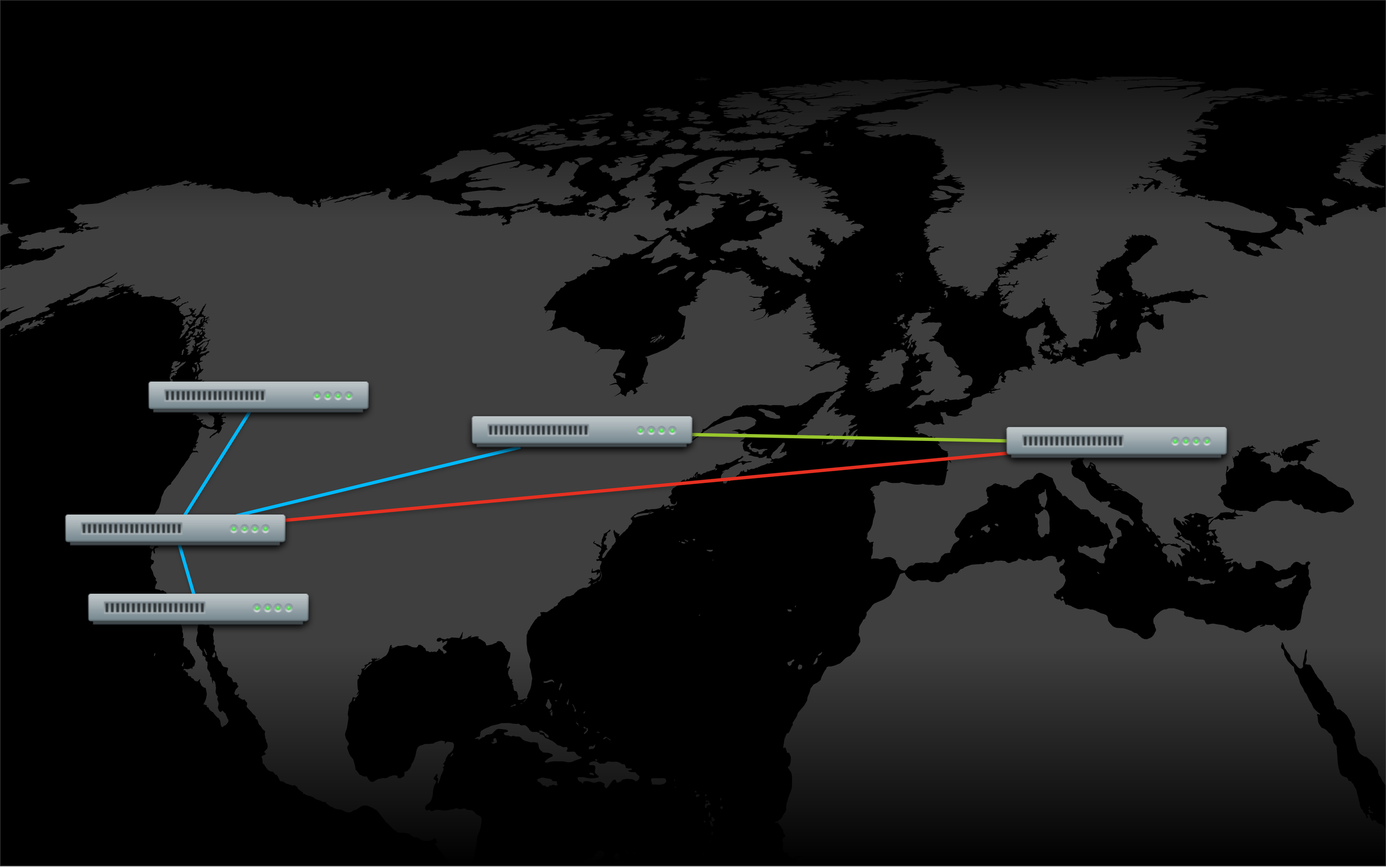


1024 Replicas

Open Directory Replication Is Serial

Dealing with Slow Links

- One slow replication link slows down replication to all replicas at that level
- Connect replicas with slow connections to a relay, not the OD master

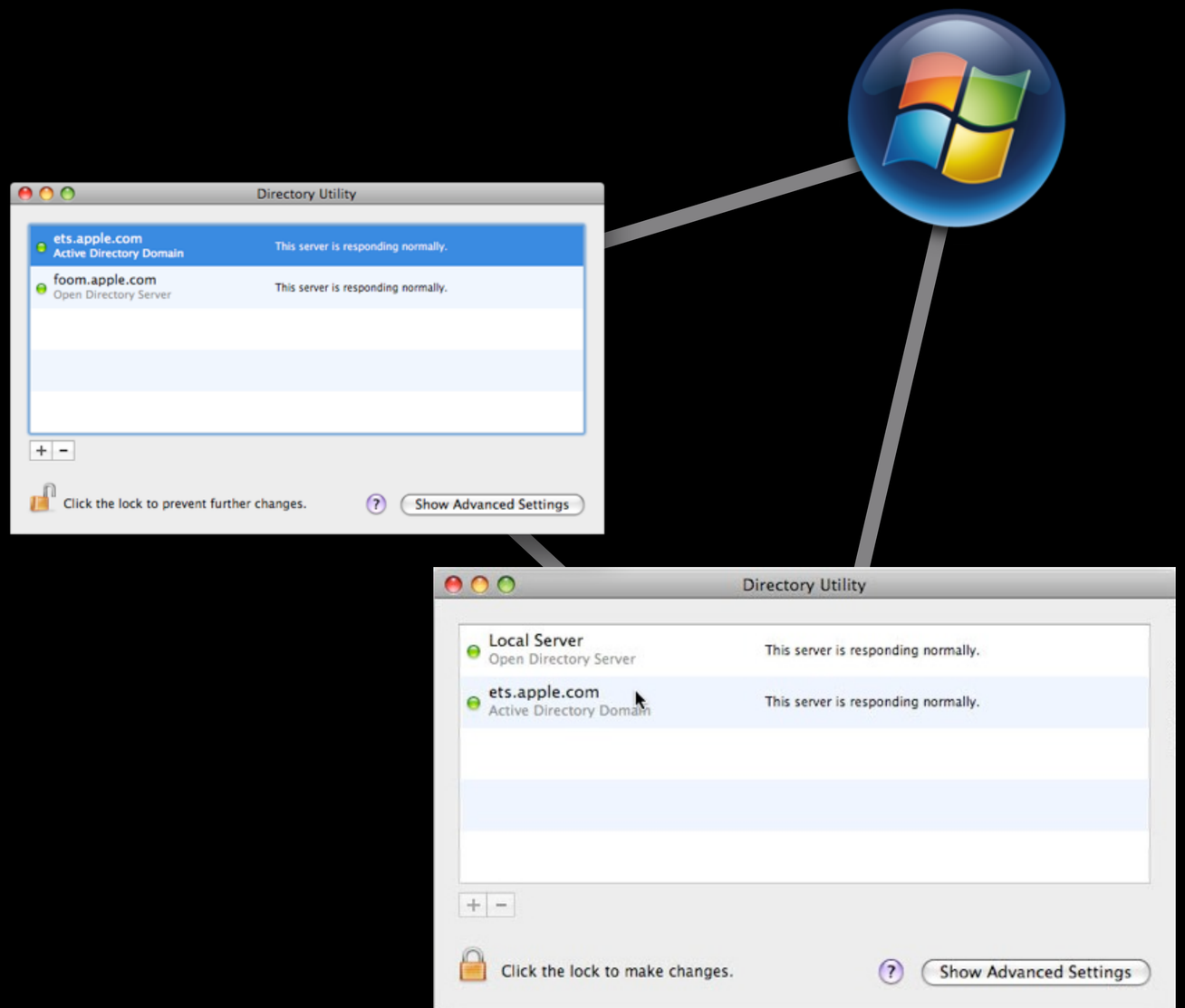


Magic Triangle

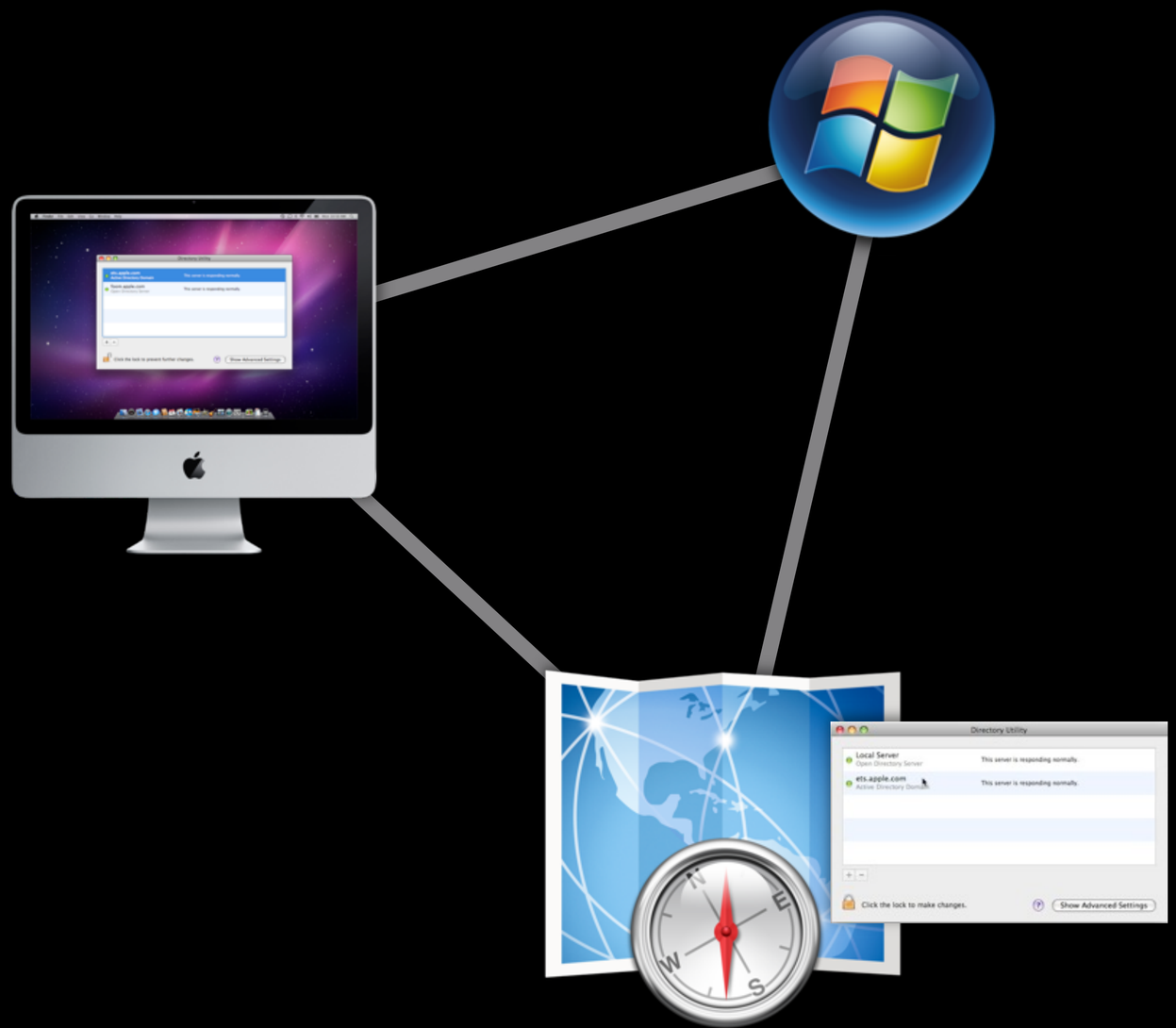
Magic Triangle Has Many Names

- Magic Triangle
- Golden Triangle
- Dual Directory
- Cylinder of Destiny
- Pyramid of Doom

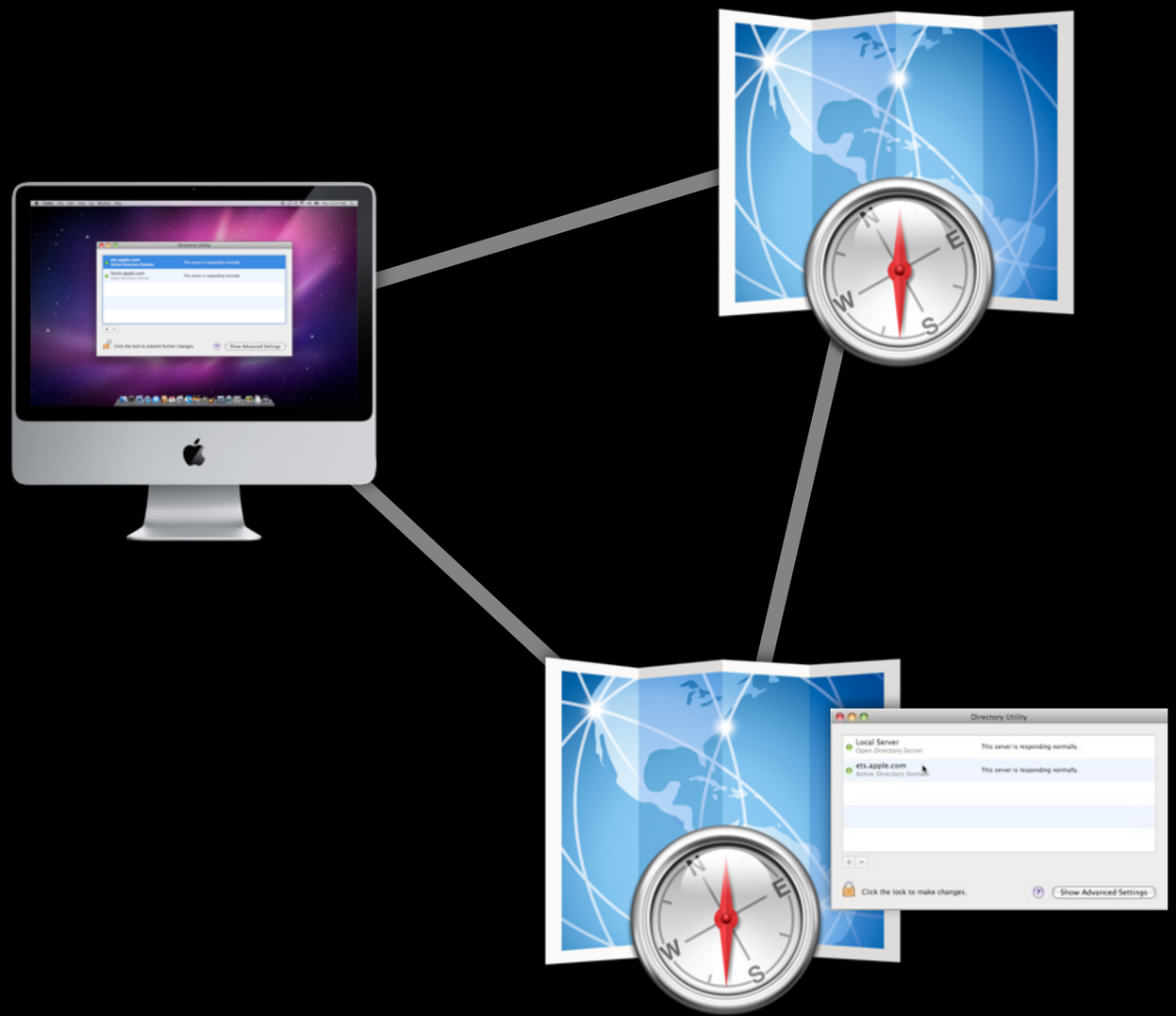
Magic Triangle



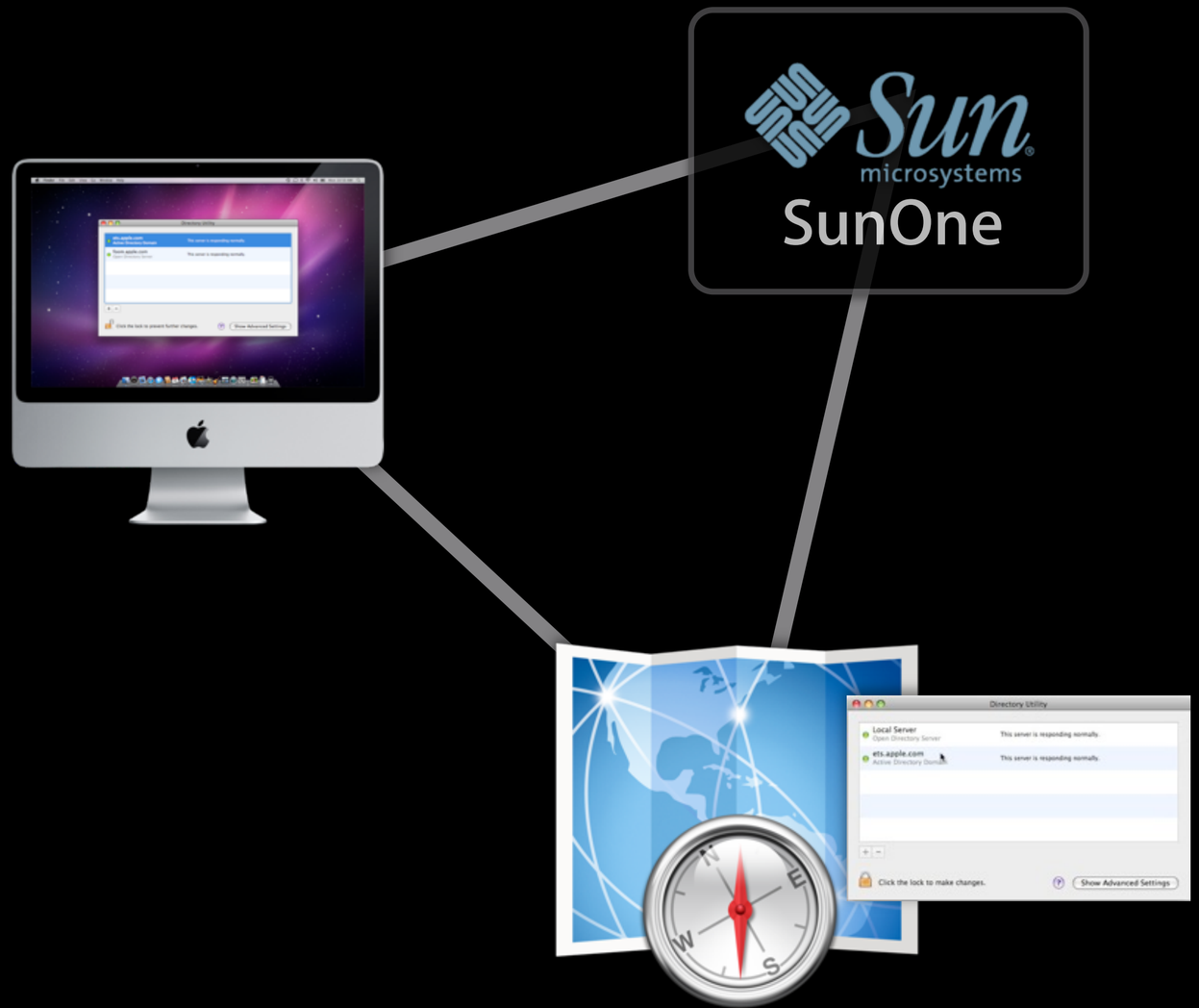
Magic Triangle Does Not Require AD



Magic Triangle Does Not Require AD



Magic Triangle Does Not Require AD



Magic Triangle Setup

- Order is important!

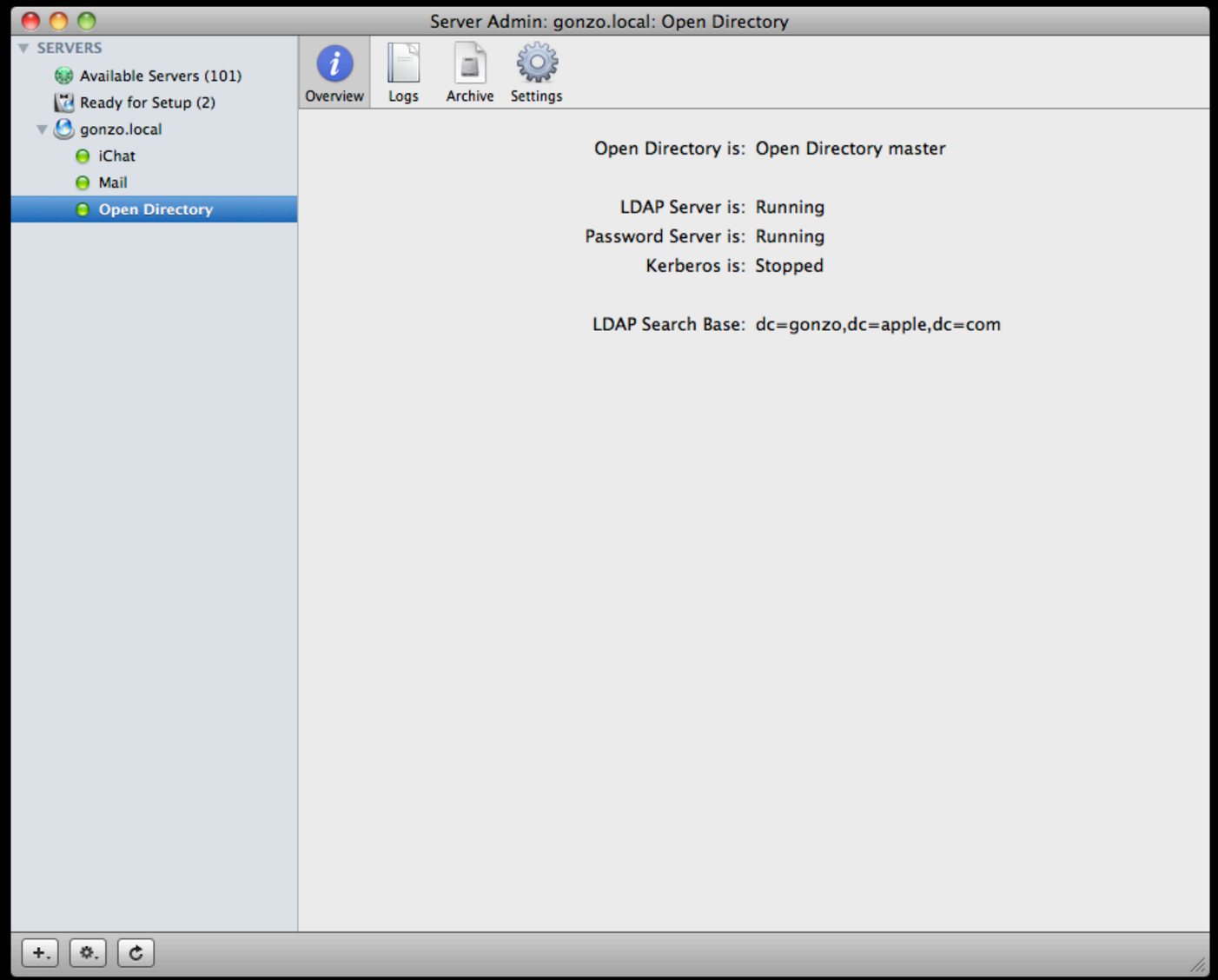
Verify your DNS config!

Magic Triangle Setup

- Order is important!
  - Verify your DNS!
    - Forward and reverse for server hostname
  - Bind to AD (or other directory) first
  - Kerberize services
  - Setup OD master

Server Admin Status

- Server admin will show kerberos as “stopped”
  - This is normal!



Best Practices

- Don’t duplicate usernames
  - Especially admin users

Changing IP and Hostnames

Steps

- Make the change in System Preferences

Verify your DNS config!

Steps

- Make the change in System Preferences
- Verify forward and reverse DNS for server
- Run changeip
- Reboot
- Run slapconfig -kerberize
- Use changedirdata.pl

For More Information

Mark Malone
Internet and Server Technologies Evangelist
mmalone@apple.com

Apple Training and Certification
http://training.apple.com

Related Sessions

Snow Leopard Server Setup: Under the Hood	Russian Hill Wednesday 9:00AM
Adding Authentication, Authorization, and Access Controls with the Open Directory Framework	North Beach Thursday 10:00AM

Labs

Directory Service Lab	Information Technologies Lab Wednesday 10:30AM
Directory Service Lab	Information Technologies Lab Thursday 2:00PM
Server Engineering Meet and Greet	Information Technologies Lab Wednesday 1:00PM

Q&A

WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

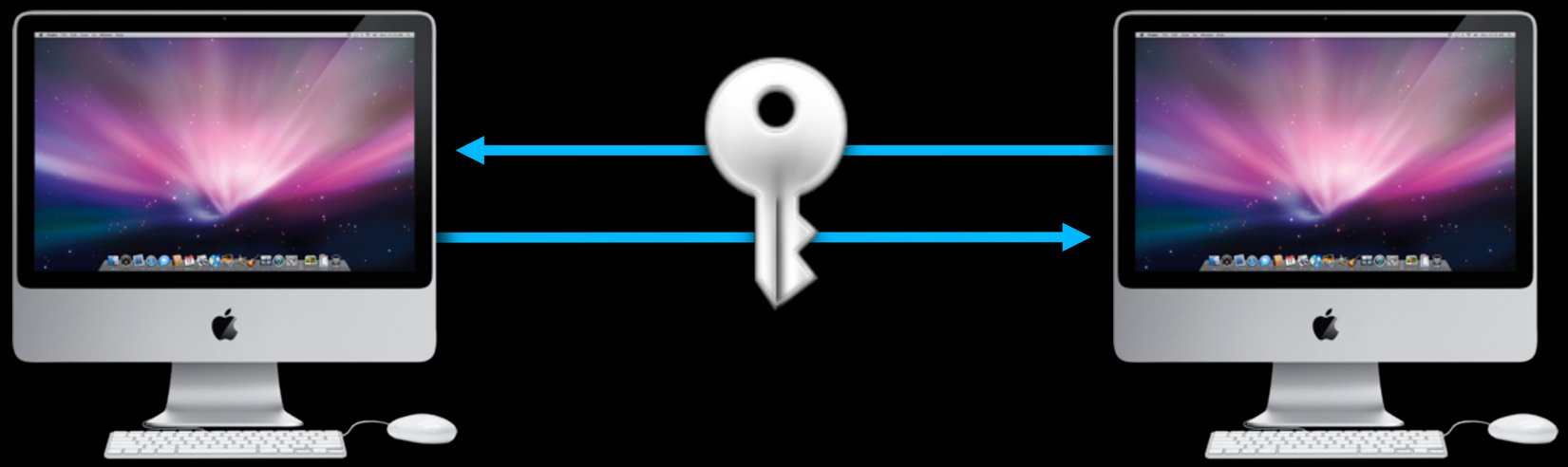
Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

WWDC09

Password Synchronization

- You need to write a tool to be called whenever a password is changed
- Install in /usr/sbin/authserver/tools/



Your Password Sync Tool

- Should accept arguments of: <username> <admin|standard>
- The password being set will be sent to stdin with a newline after
- You can now do whatever you need to do to synchronize
- Use secure methods to send the password elsewhere!
  - Kerberos
  - SSL

Enabling Password Synchronization

- Disabled by default
- Specify your command as the ExternalCommand in /Library/Preferences/com.apple.passwordserver.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>BadTrialDelay</key>
	<integer>0</integer>
	<key>Debug Log Options</key>
	<dict>
		<key>Change List</key>
		<false/>
		<key>Quit Command</key>
		<false/>
	</dict>
	<key>DeleteWaitInMinutes</key>
	<integer>2</integer>
	<key>ExternalCommand</key>
	<string>Disabled</string>
	<key>KerberosCacheLimit</key>
	<integer>95000</integer>
```

Enabling Password Synchronization

- Disabled by default
- Specify your command as the ExternalCommand in /Library/Preferences/com.apple.passwordserver.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>BadTrialDelay</key>
	<integer>0</integer>
	<key>Debug Log Options</key>
	<dict>
		<key>Change List</key>
		<false/>
		<key>Quit Command</key>
		<false/>
	</dict>
	<key>DeleteWaitInMinutes</key>
	<integer>2</integer>
	<key>ExternalCommand</key>
	<string>mytool</string>
	<key>KerberosCacheLimit</key>
	<integer>95000</integer>
```